REMARKS/ARGUMENTS

The Applicant respectfully reiterates the arguments presented in the amendment dated July 8, 2004 and respectfully submits that the claimed invention is patentable over *Winslett et al.* for at least the reasons already submitted. The undersigned respectfully disagrees with the Examiner's general assumption that communication requires negotiating a privacy agreement that governs the exchange of private information (Final Office Action, page 2). Furthermore, it should be noted that the Applicant has NOT broadly claimed negotiating an agreement. The claimed invention recites: negotiating a privacy agreement that governs the exchange of private information. As such, it is respectfully submitted that Examiner's adoption of the broadest dictionary definition of the word "agreement" to summarily reject the claimed invention is improper. Still further, it is respectfully submitted that Examiner's general assumption that a handshake involved in establishing a communication protocol implicitly teaches: establishing an authorization privacy agreement, and accepting a proposed privacy agreement, is improper (see, arguments (C) and (D) below). Moreover, contrary to the Examiner's assertion, it is respectfully submitted that a "hand shake" between two parties to establish a "communication agreement," cannot possibly teach or suggest negotiating a privacy agreement by proxy server with a server on behalf of a client because a two party communication, clearly, lacks an third party which would be required when a first party negotiates an agreement with a second party on behalf of a third party.

Nevertheless, solely in order to expedite prosecution, claims have been further amended to recite additional patentable features. More particularly, claims have been amended to additionally recite: examining at least one proposed privacy agreement that governs that exchange of privacy information associated with a client (see, for example, Fig. 9A, operation 916) and generating an accepted privacy agreement that includes one or more components that define the accepted privacy agreement (see, for example, specification page 17-19).

In the Final Office Action, the Examiner has admitted that *Winslett et al.* fails to even teach that a privacy agreement is received form a server device (Final Office

Action, page 12). Accordingly, it is respectfully submitted that it should be evident that *Winslett et al.* cannot possibly teach any one of the additional features of: (a) examining at least one proposed privacy agreement, (b) and generating an accepted privacy agreement that includes one or more components that define the accepted privacy agreement, (c) negotiating at least one component of at least one proposed privacy agreement when it is determined that a privacy agreement should not be accepted, and (d) negotiating a privacy agreement by the proxy server on behalf of a client device when not in accord with an authorization agreement;

In Final Office Action, the Examiner has rejected the claims as being anticipated by or obvious in view of "Assuring Security and Privacy for digital library transactions on the web: client and sever security policies," by Winslett et al. (*"Winslett et al."*). This rejection is fully traversed below.

Rejection of claims under 35 U.S.C. 102

In the Office Action, the Examiner has rejected claims 1-7, 9-23 and 34-36 under 35 U.S.C. 102 (b) as being anticipated by *Winslett et al.*

(a) Winslett et al. does not teach or suggest: negotiating a privacy agreement

It is noted that *Winslett et al.* states that a personal security assistant helps a client obtain credentials, stores them locally, attaches them to service requests in accordance with the policies established by the client, and determines what credentials are needed for a particular service request (*Winslett et al.*, page 142, 1st Col., 1st paragraph).

However, it should be evident that credentials referred to be *Winslett et al.* (e.g., job title, ID number, driver's license) may potentially include private information (please, see section 2, credential formats). As a result, private information may be exchanged as credentials when the methodology described by *Winslett et al.* determines that private information is needed. Determining what credentials are needed as described by *Winslett et al.*, however, does NOT teach or suggest negotiating a privacy agreement that governs the act of exchanging private information itself. Instead, *Winslett et al.*

merely teaches determining what credentials are needed and providing them as needed, rather than providing all of the credentials at once.

It is also noted that *Winslett et al.* states that "an extra round of communication" with the server may be required to determine by the personal security assistant what credentials are required for a particular request (*Winslett et al.*, page 142, 2nd column, 1st full paragraph). However, it is very respectfully submitted that performing "an extra round of communication" does NOT teach or suggest negotiating a privacy agreement that governs the act of exchanging private information. Clearly, this "extra round of communication" is performed solely to determine what credentials are required by one party to service a particular request (*Winslett et al.*, page 142, 2nd column, 1st full paragraph). Even from a very broad perspective, however, performing "an extra round of communication" to determine what credentials are needed does NOT teach or suggest negotiating an agreement that will govern the exchange of information because, among other things, there is no need or desire in *Winslett et al.* with respect to a negotiation or a privacy agreement. More particularly, *Winslett et al.* does NOT even remotely suggest that an extra round of communication should be used to negotiate anything.

As will be appreciated, a privacy agreement may be a formal agreement (e.g., a document in a markup language (see, for example, Specification, page 17-19). As such, a privacy agreement, among other things, can serve as a legally binding agreement between two parties. Similar to a legal agreement, a privacy agreement may offer both parties protection, and serious consequences may result if an agreement is violated. Clearly, the methodology of *Winslett et al.* does not teach or suggest negotiating a privacy agreement that governs the exchange of information. As a result, the methodology of *Winslett et al.* does NOT offer many advantages that a privacy agreement which has been negotiated can provide.

Furthermore, even assuming purely for the sake of argument that performing "an extra round of communication" in the context of the methodology of *Winslett et al.* somehow remotely suggests negotiating a privacy agreement, *Winslett et al.* would NOT enable one of ordinary skilled in the art to negotiate a privacy agreement which governs the exchange of private information. It should be noted that the specification, among other things, provides an illustrative example of an accepted privacy agreement in accordance with one embodiment of the invention (Specification, page 17-19). As

noted in the specification, a privacy agreement can, for example, be negotiated in accordance with Platform for Privacy Preferences (P3P) and provided as a document in a markup language (e.g., XML, HTML, WML, and HDML).

Accordingly, it is respectfully submitted that the *Winslett et al.* lacks a fundamental teaching, namely, a privacy agreement and cannot possibly teach or suggest the invention recited in claim 1. In addition, it should be evident that *Winslett et al.* does NOT teach negotiating a privacy agreement before private information is exchanged. Thus, claim 1 is patentable over *Winslett et al.* for an additional reason.

***(b) Winslett et al.* does not teach or suggest: determining whether a privacy agreement is needed**

Contrary to the Examiner's assertion, it is respectfully submitted that "determining what credentials are needed" does NOT teach or suggest determining whether a privacy agreement is needed (see, for example, claim 1). Firstly, matching credentials of one entity to the requirement of another entity in itself does NOT necessarily mean that there is an agreement between the two entities which governs the exchange of information between them. Also, exchanging information in one or more instances between two parties does not necessarily mean that there is an agreement or a need for an agreement between them. More particularly, determining what credentials one party requires does NOT teach or suggest determining whether a privacy agreement is needed. As such, it is respectfully submitted that *Winslett et al.* cannot possibly teach or suggest (b) determining whether a privacy agreement is needed before private information is exchanged (claim 1).

Independent claims 9, 19, 34, 35 and 36 recite one or more similar features as discussed above with respect to claim 1.

***(c) Winslett et al.* does not teach or suggest :establishing an authorization agreement**

Moreover, some of the independent claims recite additional features that render them patentable over *Winslett et al.* for additional reasons. For example, claim 9 recites establishing an authorization agreement that enables a proxy server to negotiate

privacy agreements with server devices on behalf of the client device. Contrary to the Examiner's assertion (Office Action, pages 3-4), it is respectfully submitted that "managing a client's credentials in accordance with stated policies" does NOT teach or suggest establishing an authorization agreement. It should be noted that *Winslett et al.* teaches managing the client's credentials in accordance with policies that are in place. The claimed invention, however, recites establishing an agreement. Thus, the methodology of *Winslett et al.* lacks a fundamental teaching, namely establishing an agreement. Clearly, *Winslett et al.* does not teach or suggest that an authorization agreement be established to enable one entity to negotiate on behalf of another entity. As such, it is respectfully submitted that *Winslett et al.* cannot possibly teach or even remotely suggest establishing an authorization agreement that enables the proxy server to negotiate privacy agreements with server devices on behalf of a client device.

***(d) Winslett et al.* does not teach or suggest: accepting a proposed privacy agreement when in accord with the authorization agreement**

Contrary to the Examiner's assertion, it is respectfully submitted that "determining what credentials are needed for a service," and a "policy on credential submission" does not teach or suggest this feature. In general, using a policy for submission of credentials does not teach or suggest accepting an agreement. Clearly, *Winslett et al.* does not teach or even remotely suggest that a privacy agreement be accepted when it is in accord with an established authorization agreement. In fact, *Winslett et al.* does NOT even remotely suggest a proposed agreement, or proposing an agreement. As such, it is respectfully submitted that *Winslett et al.* cannot possibly teach or suggest accepting a proposed privacy agreement as a privacy agreement by a proxy server for a client device when in accord with an authorization agreement (claim 9).

***(e) Winslett et al.* does not teach or suggest: negotiating a privacy agreement by a proxy server for a client device when the authorization agreement is not in accord with the authorization agreement**

In addition, it is respectfully submitted that contrary to the Examiner's assertion, "submitting credentials which may require another round of communication" (Office Action, page 5-6) does not teach or even remotely suggest negotiating a privacy

agreement by a proxy server for a client device when not in accord with the authorization agreement (claim 10).

It should be noted that the Examiner has noted that *Winslett et al.* fails to explicitly disclose that a privacy agreement is received from a sever device (Office Action, page 9). As such, the rejection of claim 9 under 35 U.S.C. 102 is improper. Nevertheless, these rejections were addressed above, and the Examiner's rejections under 35 U.S.C. 103 are also addressed below.

Rejection of claims under 35 U.S.C. 103

In the Office Action, the Examiner has rejected claims 8-18, 25-26, 31-33 and 35 under 35 U.S.C. 102 (b) as being obvious over *Winslett et al.*

***(f) Winslett et al.* does not teach or suggest: accepting the proposed privacy agreement when in accord with the authorization agreement, or negotiating the privacy agreement when not in accord with the authorization agreement**

As noted above, *Winslett et al.* does not teach or suggest these features. The Examiner has noted that *Winslett et al.* fails to explicitly disclose that a privacy agreement is received from a server device (Office Action, page 9). However, the Examiner seems to asserting that "meeting a list of qualifications which the server must meet before the client does business with the server" is equivalent to receiving a proposed privacy agreement which may be accepted (see, for example, claim 9). The Applicant very respectfully disagrees because "determining whether a list of qualifications has been made" does NOT teach or suggest: receiving a proposed privacy agreement that may be accepted or further negotiated. Clearly, no agreement (e.g., formal document) is received by any entity in *Winslett et al.*

Again, it is respectfully submitted that the methodology of *Winslett et al.* lacks several fundamental teachings which include: negotiating an agreement, establishing an agreement, giving authority to one entity to negotiate an agreement on behalf of an other entity. Clearly, *Winslett et al.* does not teach or suggest that an authorization agreement be established to enable one entity to negotiate on behalf of another entity.

Also, *Winslett et al.* fails to teach or even to remotely suggest accepting a proposed privacy agreement when in accord with an authorization agreement (claim 9) or negotiating the privacy agreement when not in accord with the authorization agreement (claim 10).

***(g) Winslett et al.* does not teach or suggest: restricting release of the information received from one entity to another entity unless a suitable privacy agreement governing the use of the information is in place**

It is noted that *Winslett et al.* states that a personal security assistant entity must also be able to export portions of its credential acceptance policy to clients who ask for explanation. However, exporting portions of a credential acceptance policy does NOT teach or suggest restricting release of information which is received from one entity (e.g., a wireless client device) to another entity (e.g., a server) unless a suitable privacy agreement governing the use of the information is in place (see claim 25).

(h) The combination of *Winslett et al.* and *Gildea* does not teach or suggest: restricting release of location information unless a suitable privacy agreement governing the use of the information is in place

Finally, it is respectfully submitted that there is no motivation or suggestion in either *Winslett et al.* or *Gildea* to restrict release of location information unless a suitable privacy agreement is in place. In the Office Action, the Examiner has asserted that one of ordinary skill in the art would have been motivated to include a location manager of *Gildea* in order to determine the location of a client (Office Action, page 12). However, it is respectfully submitted that this assertion does not address the lack of a suggestion or a motivation in the cited art to restrict release of location information unless a suitable privacy agreement is in place (see, for example, claim 28). Moreover, it is respectfully submitted that *Winslett et al.* and *Gildea,* taken alone or in any proper combination thereof, does not teach or remotely suggest restricted release of location information unless a suitable privacy agreement is in place.

Conclusion

Based on the foregoing, it is submitted that claims are patentably distinct over the cited art of record. Additional limitations recited in the independent claims or the dependent claims are not further discussed because the limitations discussed above are sufficient to distinguish the claimed invention from the cited art. Accordingly, Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner.

Applicant hereby petitions for an extension of time which may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 500388 (Order No. UWP1P026). Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

R. Mahboubian
Reg. No. 44,890

P.O. Box 70250
Oakland, CA 94612-0250
(650) 961-8300